Cisco prédit la multiplication des attaques de destruction massive

NotPetya (ou ExPetr), le faux ransomware qui s'attache à détruire les ordinateurs infectés comme l'ont constaté nombre d'entreprises dont Saint-Gobain, Mondelez, Maersk ou encore Reckitt Bensicker, est-il un avant goût d'un phénomène appelé à s'ancrer dans le quotidien des RSSI ? Cisco en est convaincu. *« Les acteurs malveillants ajoutent des tours nouveaux et sophistiqués à leurs exploits*, avance David Ulevitch, vice-président et responsable sécurité chez l'équipementier américain. *Leur objectif n'est pas seulement d'attaquer, mais de détruire d'une manière qui empêche les défenseurs de restaurer les systèmes et les données. »* Une nouvelle tendance que Cisco baptise **DeOS pour « Destruction of services »**.

Ce constat est issu du rapport d'étape de milieu d'année sur la sécurité, le Midyear Cybersecurity Report (MCR), que le spécialiste réseau vient de publier. *« Beaucoup des tendances de sécurité que nous explorons dans le MCR s'attaquent à l'émergence future de DeOS »*, insiste son superviseur qui rappelle que le rapport est un travail réalisé avec nombre de partenaires comme Rapid7, Qualys, Radware, RSA ou Flashpoint. Autrement dit, il faut s'attendre à d'autres attaques à la NotPetya, après laquelle il reste visiblement impossible de récupérer les données touchées (sauf dans certains cas).

Des DDoS à 1 Tbit/s

Si le pire semble donc à venir, les campagnes d'infections actuelles sont déjà très dangereuses pour les organisations, que l'on parle d'attaques DDoS ou d'usage de nouveaux malwares. Elles démontrent notamment la capacité qu'ont leurs auteurs à s'adapter à la situation. *« Dans leur bataille pour gagner du temps et de l'espace pour opérer, les adversaires restent à la recherche de moyens d'échapper à la détection, en général par une approche qui change rapidement lorsque certaines tactiques ne fonctionnent pas »*, indique David Ulevitch. Dans certains cas, les attaquants abandonnent ainsi les outils les plus récents, comme des kits d'exploitation, pour revenir à des méthodes plus éprouvées (compromission de courrier électronique d'entreprise ou ingénierie sociale).

Le rapport (dont on peut avoir un large aperçu en images) revient ainsi sur les attaques DDoS, notamment celles propagées par les objets et systèmes connectés *« qui n'ont pas été conçus pour se protéger des cyberattaques ; les criminels en profitent pour exploiter cette myriade de failles de sécurité »*. On l'a vu en fin d'année dernière avec le botnet Mirai qui a lancé des attaques à plusieurs centaines de Gbit/s. Pour Cisco, juste un apéritif. *« Nous sommes entrés dans ce que l'on appelle maintenant « l'ère DDoS 1-Tbit/s », où les charges DDoS pilotées par IoT peuvent provoquer des attaques de grande envergure susceptibles de perturber l'Internet lui-même »,* écrit la firme.

Des attaques plus sournoises

Si l'usage des kits d'exploitation recule à cause de leur manque de discrétion, les méthodes d'activation d'une attaque évoluent de manière de plus en plus sournoise. *« Certains attaquants utilisent des systèmes de distribution de malwares qui obligent les utilisateurs à déclencher eux-mêmes la*

menace, résume le responsable sécurité. *Ce faisant, [les attaquants] évitent la détection, car les logiciels malveillants ne peuvent pas être identifiés dans une sandbox.* » Qui plus est, les cybercriminels ont également tiré avantage du Cloud en développant des plates-formes Ransomware-As-A-Service (RaaS) *« qui permettent d'entrer rapidement dans le lucratif marché du ransomware »*. La nouvelle génération des kits d'exploitation en quelque sorte.

Dans cet océan de menaces, quelques points positifs émergent. Dont le raccourcissement considérable du temps de détection des attaques. Il était d'un peu plus de 39 heures en 2015, selon Cisco. Entre novembre 2016 et mai 2017, il est tombé à 3,5 heures. Une évolution appréciable qui ne fera néanmoins que pousser les cybercriminels à être plus efficaces. Et les marchands de sécurité à mettre toujours plus en avant leurs solutions de protection.

Lire également

Guillaume Poupard, Anssi : « NotPetya, c'est de la médecine de guerre »

WannaCry et NotPetya laissent-ils les DSI de glace ?

Petya : un lien avec la France et un acte de guerre selon l'OTAN